Background

Home and corporate users in ever-increasing numbers are using wireless networks based on the 802.11b, 802.11a, 802.11g and the emerging 802.11x/i/n standards. In March 2003, the Gartner Group reported that there were 4.2 million frequent users of wireless local area networks (LAN) and predicted that number to grow to 31.7 million users by 2007. This same group further indicated that approximately 30 percent of all companies with a computer network have some kind of wireless network, either official or rogue.

Popular small office, home office (SOHO) equipment, such as the Linksys WRT54G Netgear WGR614 and D-Link DI-24 have begun to appear on Navy networks as rogue access points (AP). As consumers of SOHO equipment have become more familiar with wireless networking, the demand for these products has increased while the price for entry-level equipment has dropped. However, this equipment does not meet the Department of Defense (DoD) or Naval Network Warfare Command (NETWARCOM) requirements for wireless usage because it does not provide adequate access control or encryption at link layer 2.

Navy and Defense Network Security Policy

In July 2004, the NETWARCOM Network Security Division (NNWC NSD) released two messages that imposed a "wireless moratorium" for both afloat and ashore network infrastructure: ALCOM 038-04 (DTG 021619Z Jul 04) and ALCOM 046-04 (DTG 191834Z Jul 04). This moratorium included but was not limited to "commercial wireless technologies and their derivatives, as standardized in IEEE standards 802.11, 802.15 and 802.16 commercial wireless devices, services and technologies and voice and data capabilities that operate either as part of the Navy enterprise network or stand-alone systems."

While these messages imposed a moratorium, they also delineated a waiver process for identifying and mitigating the risks associated with wireless networks that were deployed under an Interim Authority to Operate (IATO) or ATO or operated without official approval by NNWC NSD. To be considered for a waiver, the information assurance manager for each network was directed to register the network and provide specific technical details to NNWC NSD no later than Aug. 30, 2004.

Upon receiving registration information, NNWC NSD reviewed each wireless network's specifications and System Security Authorization Agreement (SSAA) to determine whether the system met the requirements of DoD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG). Each wireless network considered for a waiver had to comply with DoDD 8100.2 and implement access control methods to be considered for a waiver. The registration and waiver process remain in effect at this time.

Federal Information Processing Standards

The information assurance triad is composed of authentication, integrity and confidentiality. DoDD 8100.2 addresses the confidentiality requirement of the IA triad by mandating encryption. The requirements of DoDD 8100.2 are straightforward and stringent, "Encryption of unclassified data for transmission to and from wireless devices is required …. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program (CMVP) as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2." Complete information about FIPS 140-2 is available at http://csrc.nist.gov/wireless/S05_NIST-tk2.pdf.

While not specifically delineated in DoDD 8100.2 or the NNWC moratorium, NNWC directed that FIPS 140-2 compliance will be at layer 2. Layer 2, or the data link layer, defines physical addressing and network topology and directs the functional and procedural means to transfer data between network entities of the Open Systems Interconnection (OSI) model. This is an important distinction because some wireless mechanisms may be FIPS 140-2 compliant at network layer 3, which provides the routing, flow control, segmentation/desegmentation and error control functions required to transmit information between networks.

Encryption at layer 2 ensures that all of the packet contents, except the data link header, are encrypted. This ensures that data and routing information are encrypted and protects access points and the computer's Internet Protocol (IP) address, as well as the media access control (MAC) address. Encryption at layer 2 can be used to ensure access control, prevent attacks on data privacy ("sniffing" of layer 2 header information) and thwart spoofing attacks.

FIPS 140-2

The National Institute of Standards and Technology (NIST) published FIPS 140-2, Security Requirements for Cryptographic Modules, May 25, 2001. This standard describes the requirements that hardware and software products should meet for sensitive but unclassified (SBU) use. FIPS 140-2 compliance is mandatory for federal agencies and has become the de facto standard for industry.

FIPS 140-2 addresses the confidentiality and integrity pieces of the information assurance triad, but it does not address access

control. There is no single standard for wireless authentication and access control; however, NNWC has deemed products such as TACACS+, RADIUS and Kerberos acceptable for controlling authentication, authorization and accounting (AAA).

It is the responsibility of the vendor to achieve certification of its cryptographic product. Certification of a product to this standard is a strong selling point within both the federal government and industry. On average, the certification process takes 15 months and costs approximately $200,000 for laboratory testing, mandatory certification documentation and follow-on changes required to meet the FIPS 140-2 standard.

The CMVP is jointly managed by U.S. federal agency, NIST, and Canada's national cryptology agency, the Communications Security Establishment (CSE). Vendors contract with one of nine independent laboratory-testing facilities. Laboratory personnel review and test products and submit validated FIPS 140-2 candidates to NIST and the CSE for certification. A graphic representation of this process is shown in Figure 1.

Once certified, the certification applies only to the version of the process that was originally submitted, all product updates must be revalidated. It is important to note that a vendor may submit an entire product or a cryptologic module for testing. A vendor may implement a FIPS 140-2 module into a product that operates in both FIPS 140-2 compliant and non-compliant modes. Information assurance managers must ensure that they understand the method of implementation.

Similarly, vendors may purchase the rights to incorporate a FIPS 140-2 certified module into their products. These products may then be labeled "FIPS inside" to indicate that a FIPS validated component has been incorporated. NIST maintains a list of approved cryptologic modules at http://csrc.nist.gov/cryptval/140-1/1401val.htm/. Products that are currently undergoing evaluation are listed on a prevalidation list at http://csrc.nist.gov/cryptval/preval.htm/.

Compliance

Navywide, relatively few wireless systems were reported to NNWC, so it is likely that not all wireless networks were reported. In March 2005, the NNWC C4I and Network Security Division jointly directed the Fleet Information Warfare Center (FIWC) Navy Red Team *(see the Red Team text box on the next page)* to complete a search for 802.11 wireless networks onboard selected Navy installations. In April 2005, the Naval Computer Incident Response Team (NAVCIRT) directed a similar action. NAVCIRT went one step further and directed the localization and identification of unapproved wireless networks operating onboard Navy installations.

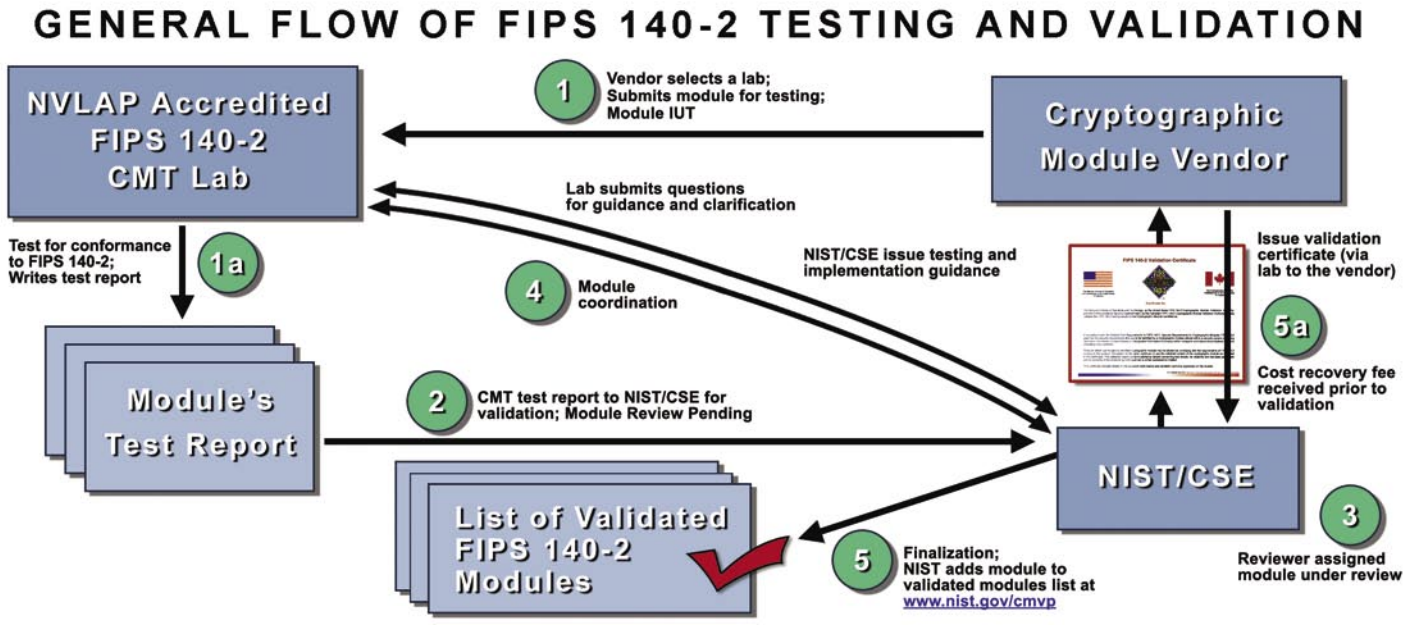
To comply with personal privacy and Title 10 concerns, and in keeping with the detection and localization effort, the Navy Red Team configured wireless equipment to capture and retain only the header information from wireless IEEE 802.11 data packets. These actions ensured that data of an attributable nature were not collected. The results of these actions are classified; however, the Navy Red Team specifically investigated any network operating with an encryption scheme that was not FIPS 140-2 certified.

Examples of unapproved encryption schemes are Wired Equivalent Privacy (WEP) and wireless fidelity (Wi-Fi) Protected Access Pre-Shared Key (WPA-PSK) encryption. This is the encryption method generally used with SOHO equipment. Neither of these encryption schemes are FIPS 140-2 certified; consequently, both may be attacked though various methods.

WEP and WPA

WEP was the original encryption scheme designed for wireless networks. WPA-PSK is an improved standard that addresses known WEP vulnerabilities. Temporal Key Integrity Protocol (TKIP) is the wireless security encryption mechanism within WPA-

Figure 1. A graphic representation of the FIPS certification process.



PSK that removes the predictability of WEP initialization vectors (IVs) in the encryption scheme. Collectively, this is known as WPA-PSK (TKIP).

An information assurance manager might wonder how serious a security risk is posed by using WEP or WPA-PSK on a Navy network. In 2001, when Scott Fluher, Itsik Mantin and Adi Shamir published "Weaknesses in the Key Scheduling Algorithm of RC4," and the Shmoo Group released the beta version of Airsnort, compromising a WEP key was a daunting task. A would-be attacker required in-depth Linux knowledge to patch and install unsupported wireless drivers, compile programs, capture a substantial amount of wireless network data, and use the poorly documented tools available.

Under the WEP 128-bit encryption scheme, 16 million keys can be generated; roughly 9,000 of these are weak (also known as interesting) due to the implementation of the IV. By capturing approximately 5 million data packets, Airsnort could "guess" most WEP keys. This number would statistically ensure collection of approximately 4,000 interesting IVs. The process of breaking WEP was time consuming because collection of these packets was dependent on network utilization. Collection time varied with wireless data network usage. However, a network with few users and moderate network usage might take two weeks of packet capture before the WEP key could be obtained.

These statistically weak or interesting IVs received wide recognition within the industry and, as a result, most vendors made changes to their WEP firmware and software implementations which filtered or removed interesting IVs. Older versions of Airsnort and other tools that attacked WEP by examining interesting IVs became unusable against most wireless equipment produced after 2002.

But even with vendor implementation changes, WEP and WPA continue to be serious security risks. Advances in the art of cracking WEP and WPA networks have made arguments for using these encryption schemes in Navy networks indefensible. The greatest advancement has been the proliferation of well-documented tools accompanied by Internet tutorials that explain the process of compiling and using the unsupported drivers required to operate wireless equipment in "promiscuous" or "monitor" mode. This mode allows an attacker to passively capture network wireless traffic and then reinject traffic into a WEP or WPA protected network.

An average Linux user can follow instructions that will guide him or her in the compilation and installation of the drivers, libraries and tools. As an alternative, an attacker may download and install precompiled components using a Linux distribution compatible with the Red Hat Package Manager (RPM) or Debian Advanced Package Tool (apt-get). Additionally, many tools that formerly ran on Linux operating systems have been ported to the Microsoft Windows operating system.

WPA-PSK is Unsuitable for Navy Networks

In 2004, a new WEP statistical cryptanalysis attack (the exploitation of weak keys) was released by Korek. While still based on the Weaknesses in the Key Scheduling Algorithm of RC4, the Korek Attack removed the requirement for the collection of interesting IVs. This attack has been coded into several tools, most notably Aircrack, WepLab and the newest version of Airsnort. Each has tool functions that slightly differ, but each tool requires far fewer packets to break WEP.

The requirement for the statistical attack is generally in the range of 500,000 to 1 million unique, as opposed to weak, IVs. While this represents a significantly smaller number of packets than in the past, network usage might dictate that a substantial amount of time before collection of the requisite number of packets had been completed. An uninformed information assurance manager might believe that security on a network with a relatively low volume of traffic may be ensured by regularly changing the WEP key before a large number of unique IVs are generated.

Aireplay negates time as a factor by allowing an attacker to inject captured encrypted packets into a wireless network. By injecting captured Address Resolution Protocol (ARP) packets,

Computer Network Defense Red Team

Red Team refers to a group of subject-matter experts tasked with playing the role of the enemy in training exercises. The purpose of Red teaming is twofold: (1) It identifies weaknesses in the defender's perimeter that would otherwise be overlooked; and (2) It gives the defenders valuable training in detecting and reacting to attacks. Properly conducted Red Team operations can identify planning shortfalls, deviations from doctrine and missed opportunities. These operations provide independent data for use in risk-management decision making. This concept has been used by the military for decades primarily in wargaming. In industry, it is often called a "peer review."

The Computer Network Defense (CND) Red Team located at the Fleet Information Warfare Center (FIWC) was created in 1996 and provides operational and exercise support to commands to improve their ability to fend off malicious computer activity. The Red Team offers many services to all levels of the Navy, from the component commander to individual commands. The FIWC Red Team is a key participant in Navy Integrated Vulnerability Assessments (NIVA). Although the Red Team is only concerned with network security testing, a typical NIVA visit includes assessments performed by a variety of teams on a host of topics such as disaster preparedness and terrorism prevention.

Navy Marine Corps Intranet (NMCI) Security Service Level Agreement (SLA) tests are performed by the Red Team under the direction of the NMCI director to ensure that the NMCI meets the security standards set forth in the contract with EDS. SLA tests are highly standardized to ensure that the results from different installations can be meaningfully compared.

The FIWC Red Team performs test and evaluation under the direction of the Navy's Operational Test and Evaluation Force (COMOPTEVFOR) and the Space and Naval Warfare Systems Command (SPAWAR) on fleet systems prior to their inception. The remainder of Red Team activities can be collectively described as special projects. Any Navy command may request FIWC assistance in testing the security of its network. This training is tailored to the needs of the individual command. Special projects can include any or all of the following elements: open source research, port scanning, remote attacks, social engineering, physical intrusion, insider attacks, and malware use and detection.

the attacker may force a reply with an unique IV. Aireplay can force the AP to generate thousands of packets per minute and provide the attacker with the requisite number of IV packets to crack WEP in a relatively short period of time.

Kismet may be the best tool for promiscuously capturing wireless network traffic. Developed by Mike "Dragorn" Kershaw, this free tool began as a wireless discovery tool and has evolved into an 802.11, layer 2, wireless network detector, sniffer and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring mode (rfmon) and can sniff 802.11b, 802.11a and 802.11g traffic. Kismet can specifically log the Transmission Control Protocol (TCP) and IV packet data required to break WEP or WPA, and it can allow data packets to be reinjected into WEP and WPA networks.

Just as filtering interesting IVs in WEP did not deliver a more secure system, WPA-PSK is also not the answer to WEP. Both WEP and WPA-PSK use a key (passphrase) that is susceptible to offline brute-force dictionary attacks. The WPA-PSK key can be between eight and 63 bytes, and SOHO implementations allow only a single PSK to be used on each wireless network. The tools WEPCrack and "dwepcrack" are capable of offline brute forcing weak WEP passwords.

Robert Moskowitz's article, "Weakness in Passphrase Choice in WPA Interface," describes a theoretical attack on WPA passwords. The tools WPA-psk-bf, CoWPAtty and WEP Crack are implementations of this attack and have demonstrated the ability to break WPA-PSK keys that are 20 characters or fewer. The Aircrack tool suite operates in an active or passive mode to gather the data required to launch these attacks. In passive mode, the Aircrack tools capture the four-packet authentication handshake between an AP and client. The handshake is then processed through a WPA breaking tool for an offline brute-force attack. If the attacker has not captured the handshake, the Aircrack tools active mode will force a disassociation and reassociation.

Threat Tools Simplified

To use the aforementioned tools, average knowledge of Linux is required to patch and install unsupported wireless drivers, compile Unix-based tools, capture network traffic and execute WEP and WPA-PSK exploits. Even with the increase in documentation and ease of compiling drivers and tools, these tasks were hurdles that had to be overcome by a novice attacker. But these barriers have all but been removed with the advent of the live Linux distribution based on the Knoppix Linux distribution. These distributions are free and distributed as an ISO. An ISO is a file that contains the complete image of a disc. These files are often used when transferring CD-ROM images over the Internet. The user simply inserts a disc into a system and powers the system on. The system will boot from the disc into a full-fledged Linux operating system.

Knoppix variants such as Auditor, Knoppix-STD (Security Tools Distribution) and Whoppix have precompiled drivers, software and cryptologic libraries that allow even a novice Linux user to launch sophisticated attacks against wired or wireless networks. Figure 2 is a screen capture from an Auditor Linux distribution.

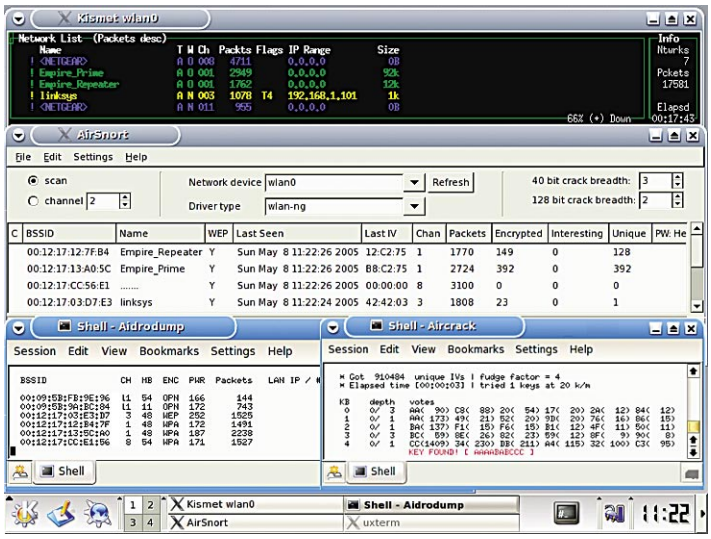


Figure 2. A screen capture from an Auditor Linux distribution. The tools Kismet, Airsnort, Airodump and Aircrack are shown running in a test environment.

The tools, Kismet, Airsnort, Airodump and Aircrack, are shown running in a test environment. An experienced Linux user could spend an hour or more reading the documentation, compiling and configuring network drivers, libraries and tools and have the ability to exploit a wireless network. I was able to download the Auditor ISO image, boot to the Auditor Linux distribution and run each of these tools within 20 minutes.

It should be apparent that powerful network attack tools to compromise WEP or WPA-PSK are freely available to anyone with an Internet connection and the ability to follow well-defined instructions. It should also be apparent that the use of wireless equipment that does not meet the requirements of FIPS 140-2, does not implement access control and has not been approved by NNWC NSD, places the entirety of Navy networks and the GIG at risk. Unapproved equipment may also become a vector for an attacker to compromise the network of a command.

The mantra, *a vulnerability assumed by one is shared by all*, definitely applies to wireless networks. An attacker could use insecure and unapproved equipment as a vector into other Navy networks or as a jumping off point into public or commercial networks, creating the false appearance that Navy personnel had launched the attack. Both NNWC and NAVCIRT are actively using the FIWC Navy Red Team to detect, localize and remove unapproved wireless networks.

Don't compromise your command or the Navy with unauthorized wireless equipment.

Cmdr. MacMichael is the Fleet Information Warfare Center (FIWC) deputy operations officer and an Information Professional (IP) officer with a master's degree in information systems technology from the Naval Postgraduate School. He has the following certifications: Certified Information System Security Professional (CISSP), GIAC Security Essentials Certification (GSEC) and Certified Wireless Network Administrator (CWNA). CHIPS